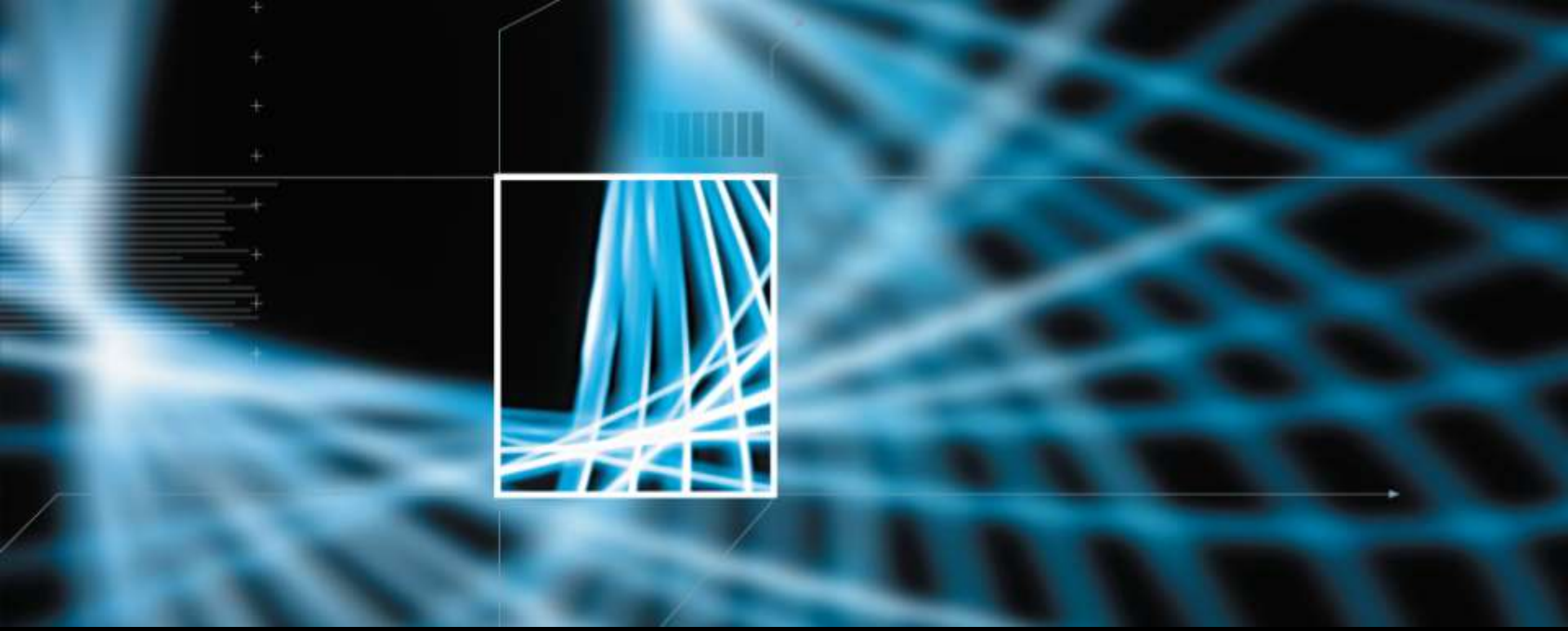


Information Sharing in the UK

Andrew Powell, Information Sharing Workshop,

Amsterdam, 16 March 2010

CPNI
Centre for the Protection of National Infrastructure

Objectives

- UK Information sharing activities
- Role of private sector
- Role of public sector
- Critique
- Input to pan-European initiatives

CPNI
Centre for the Protection of National Infrastructure

Why Share Information

- 1+1>0
- Need: much infrastructure is privately owned and operated
- Regulation is a blunt instrument
- Sharing promotes agility to change
- Added value for all

CPNI
Centre for the Protection of National Infrastructure

The Ingredients for sharing

- A basis for trust
  - Openness
  - Confidentiality
  - Honesty
  - Regular contact
- Information sharing protocol

CPNI
Centre for the Protection of National Infrastructure

What the UK is sharing

- **Risks and their mitigation**
- Private sector-to-private sector security incident and vulnerability information
- Private sector-to-public sector confidential incident and vulnerability reporting where public sector can *respond and warn*
- Public sector issued good practices and incident and vulnerability alerts
  - Has to be relevant to the UK's Critical Infrastructure Protection (CIP)
  - Based on partnership with private sector

CPNI
Centre for the Protection of National Infrastructure

UK's Information Sharing Initiatives

- **Information exchanges**
- Information sharing portals
- Warning, advice and reporting points
  - http://www.warp.gov.uk/
- Support for international groups and projects
- Other information sharing activities

CPNI
Centre for the Protection of National Infrastructure

Information Exchange Structure

- Trusted group of private sector and public sector representatives
- Rules of membership
- No cost to members
- 2 members per organisation
- Cannot delegate outside of prime and deputy members
- Information sharing protocol

CPNI
Centre for the Protection of National Infrastructure

Information Exchange Structure

- Private sector and public sector co-chairs
- CPNI co-ordinator generally
- CPNI hosted generally
- Always face-to-face meetings
- Supported by email and members only extranet web pages
- Some information exchanges have working groups which develop good practice

CPNI
Centre for the Protection of National Infrastructure

Information Exchange Structure

- New members elected by all members
- Shared area on extranet for all information exchanges
- Joint information exchange sharing day in 2008
- Access to security advice documents from CPNI

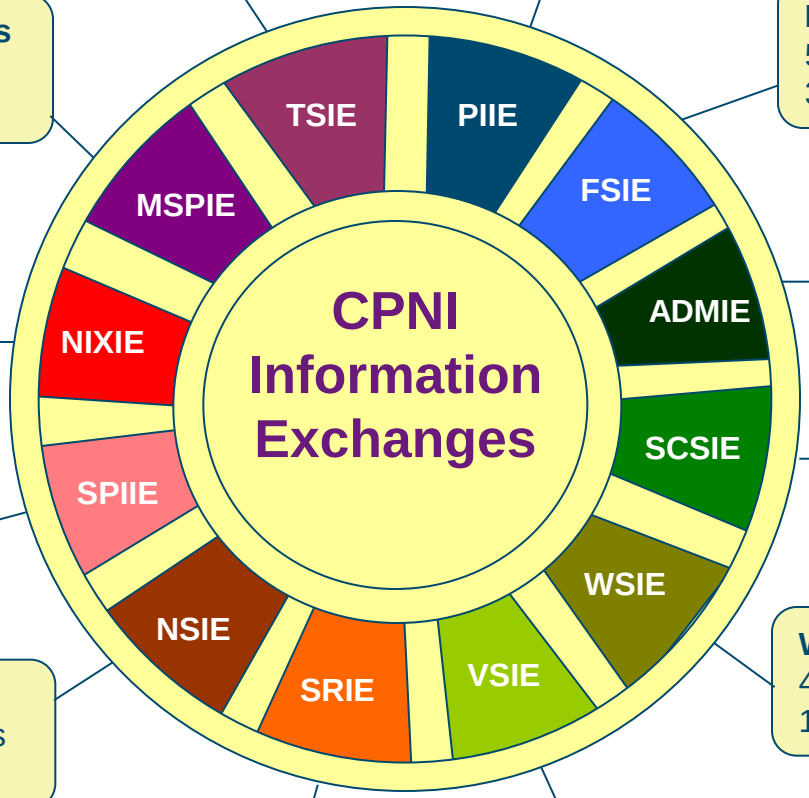
CPNI
Centre for the Protection of National Infrastructure

Information Exchange History

- First one established in 2003 using the model of the US Network Security Information Exchange
- Currently 12 information exchanges
- Based on sector, technology or activity
- Trust can take up to 2 years to establish

CPNI
Centre for the Protection of National Infrastructure

Information Exchanges



Transport Sector
28 Representatives
18 Companies

Pharmaceuticals Private sector
12 Representatives
7 Companies

Managed Service Providers
36 Representatives
23 Companies

Finance Sector
54 Representatives
34 Companies

Northern Ireland Cross sector
26 Representatives
14 Companies

Aerospace/Defence
32 Representatives
17 Companies

SCADA
77 Representatives
37 Companies

Space Industries
10 Representatives
7 Companies

Water Security
40 Representatives
18 Companies

Network Security
27 Representatives
15 Companies

Security Researchers
30 Representatives
15 Companies

Vendor Security
23 Representatives
15 Companies

12 Exchanges

220 Companies

CPNI
Centre for the Protection of National Infrastructure

Information Exchange Working Groups

- Across information exchanges. Published papers on:
  - Ethernet switches
  - Outsourcing
  - Protecting data centres
  - Server virtualisation

CPNI
Centre for the Protection of National Infrastructure

International Activity

- CPNI supports EP3R and other European Commission initiatives
- CPNI supports ENISA initiatives
- CPNI contributes to international CSIRT groups such as the European Government CSIRTs group and FIRST
- CPNI contributes to MERIDIAN, an international Public sector CIIP group using a traffic light information sharing protocol

CPNI
Centre for the Protection of National Infrastructure

International Activity

- CPNI supports the International CIIP directory
- CPNI participates in the European SCADA and Control Systems Information Exchange (e-SCSIE)
- CPNI promotes the formation of Warning, Advice and Reporting Points (WARPs) and Information Exchanges

CPNI
Centre for the Protection of National Infrastructure

Other Information Sharing Activities

- CPNI participates in information sharing groups nationally and internationally
- CPNI tries not “to re-invent the wheel”
- CPNI provides advice on setting up information sharing groups to UK organisations

CPNI
Centre for the Protection of National Infrastructure

Role of Private Sector

- Private sector form the primary membership of the exchange
- Private sector sets the direction of the exchange
- Private sector brings knowledge of good practice
- Private sector knows what can be achieved

CPNI
Centre for the Protection of National Infrastructure

Role of Public Sector

- Public sector provides the trusted environment
- Public sector has specialist knowledge
  - Policy/Laws/Regulations
  - Hazards/Threat/Vulnerabilities
- Public sector can represent a consensus position

CPNI
Centre for the Protection of National Infrastructure

Information Exchange Critique

- Establishing and maintaining trust is key
- Not scalable to large groups
- Must be face-to-face
- Large groups undermine trust
- Change of membership (“churn”) undermines trust
- Non-contribution (“lurking”) undermines trust

CPNI
Centre for the Protection of National Infrastructure

Possible Futures

- To address scalability:
  - Federated information sharing structures
  - Group of all information exchanges
- To address legal and regulatory changes:
  - Agree system of internal need-to-know controls so that law makers and regulators can be aware of problems without penalising honesty of participants

CPNI
Centre for the Protection of National Infrastructure

Possible Futures

- To address balance between need-to-know and need-to-share:
  - Education that AMBER means that you should share within your company
  - More GREEN information on organisational intranets.

CPNI
Centre for the Protection of National Infrastructure

Application to Pan-European Initiatives

- National information sharing groups
- Information sharing protocol
- Knowledge transfer from mature national initiatives
- Sharing between member states
- Facilitation by ENISA (“providing the trusted environment”)

CPNI
Centre for the Protection of National Infrastructure

Application to Pan-European Initiatives

- Good practice outputs
- Addressing the regulatory challenges
  - Dialogue with private sector
- Awareness of key common risks
- A plan to address those risks

CPNI
Centre for the Protection of National Infrastructure

Questions

- Contact:
  - Andrew Powell
  - andrewp@cpni.gsi.gov.uk
  - http://www.cpni.gsi.gov.uk

CPNI
Centre for the Protection of National Infrastructure